Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	)	WC Docket No. 16-106

COMMENTS OF THE STATE PRIVACY AND SECURITY COALITION

Jim Halpert
Anne Kierig
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

July 5, 2016

I. INTRODUCTION

The State Privacy and Security Coalition, Inc., a coalition of 25 leading communications, technology, retail, and media companies and six trade associations, respectfully submits these reply comments to the Notice of Proposed Rulemaking in the matter of "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services" (the "Proposed Rules" or "NPRM").

Comments from the defenders of the Proposed Rule do not undermine the SPSC's opening comments. Claims that all Internet service provider ("ISP") data is sensitive or should be considered sensitive fail, for reasons explained in Section II of these comments. The Commission should modify the scope of its proposed security and breach notification rules and rely on a general reasonableness standard. Similarly, as outlined in Section III of these comments, there are compelling reasons for the Commission to modify its proposed data security and data breach notification requirements so they are consistent with the approach taken by the Federal Trade Commission ("FTC") and the vast majority of state statutes.

II. SCOPE AND SUBSTANTIVE REQUIREMENTS

Both the FTC and the overwhelming majority of commenters support the State Privacy and Security Coalition's comments that sensitivity of data elements needs to be at the core of the final rule's security provisions and is missing from them now.[1] The FTC staff comments, which were adopted by a unanimous bipartisan vote of the Commissioners, agree with the central theme of the SPSC comments, emphasizing that the final Rule should be recast to distinguish between

[1] *E.g.*, Comments of FTC Commissioner Maureen K. Ohlhausen, WC-Docket 16-106 (May 27, 2016), at p. 2; Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, pp. 20-22; Comments of the Future of Privacy Forum, WC Docket No. 16-106, at 27 (May 27, 2016); Comments of Hughes Network Systems, LLC, WC Docket 16-106, at 4 n.11 (May 27, 2016); Comments of the National Cable & Telecommunications Association, WC Docket No. 16-106, at 44 (May 27, 2016).

sensitive and non-sensitive data.[2] This approach is also consistent with many other established frameworks, including the Organization for Economic Cooperation and Development ("OECD") Privacy Guidelines,[3] the National Institute of Standards and Technology ("NIST") Cybersecurity Framework,[4] and International Organization for Standardization ("ISO") security standards, which distinguish between sensitive or risky and non-sensitive information.

The NPRM proposal categorically treats all Customer Proprietary Network Information ("CPNI") and customer proprietary information as sensitive and suggests they all be subject to detailed access and use record keeping requirements. New America's Open Technology Institute ("OTI") and several other public interest groups suggest still more extensive security requirements for this data, including prescriptive encryption, password protection and data minimization requirements.[5] However, much of the information that service providers hold is not sensitive; only information that creates risk of fraud or identity theft or otherwise fits the FTC privacy framework list of sensitive data elements should require notice or heightened security measures. The FTC's comments specifically note that sensitive information should be subject to an opt-in rule and that not all information, if breached, should warrant a notification.[6]

The 47 state data security and data breach notice laws apply to the name of a state resident plus a sensitive data element. The sensitive data elements vary by state, but include social security number, government identification number, financial account number in combination with a code to access a financial account, and in some states medical information,

---

[2] Comments of Staff of the Bureau of Consumer Protection of the Federal Trade Commission In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, pp. 20-22.
[3] *See., e.g.*, OECD Privacy Framework at 16 ¶¶ 15(a)(ii), 18 (2013), *available at* https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
[4] NIST, Framework for Improving Critical Infrastructure Cybersecurity (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[5] *See e.g.*, Comments of New America's Open Technology Institute In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, WC Docket No. 16-106, p. 41 (May 27, 2016).
[6] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at p. 20.

health insurance claim information or user name and password for an online account.[7] States have considered and uniformly rejected proposals to require notification of all personally identifiable information,[8] of websites visited by state residents,[9] and long lists of data elements,[10] all of which would be swept into the NPRM's customer proprietary information definition and require notification in the case of a breach.

Furthermore, the proposed rules appear to imply a strict liability that would make the ISP the insurer of security for all information that is "linked or linkable" to a customer. The FTC comments, by contrast, state that a breach standard should be based on whether the ISP acted reasonably[11] and should be limited to situations where there may be real harm.[12] As our Opening Comments explain, imposing a checklist of prescriptive security requirements would be contrary to the FTC framework and widely accepted industry standards.

III. BREACH NOTIFICATION

There is little in the record in defense of the security portions of the proposed rule. One commenter, OTI claims that as gatekeepers, ISPs have privileged access to a comprehensive amount of customer information that customers must share with them to gain Internet access.[13] The commenter asserts that ISP customers share private information with ISPs in the narrow context of facilitating provision of Internet access, and information used outside of this context

[7] *See, e.g.*, Cal. Civ. Code § 1798.82(h) (defining "personal information").
[8] Nevada AB 0179 (2015).
[9] Illinois SB 1833 (2015).
[10] *See e.g.*, Kentucky HB 581 (2010).
[11] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, pp. 27-28, "However, the proposed rule text would impose strict liability on companies for "ensuring" security. FTC Staff suggests modifying the language to require BIAS providers to "ensure the *reasonable* security, confidentiality, and integrity of all customer PI . . . ."
[12] *Id* at p. 32.
[13] Comments of New America's Open Technology Institute, p. 3.

should be viewed as likely inconsistent with the context of initial disclosure.[14] These arguments closely mirror language in the Proposed Rule.[15]

First, OTI's comments rely heavily on what it posits as "a special duty" created by Section 222(a) to secure customer data. A plain reading of the statute shows that these arguments are inflated. Section 222(a) on its face is limited to CPNI, which is defined in the statute as relating to telephone service. What is more, Section 222(a) establishes the duty to "protect the confidentiality" of CPNI. Dozens of federal or state data security laws require "protect[ing] the confidentiality" of data,[16] and nothing about this obligation gives the FCC a reason to impose extraordinarily specific information security or extraordinarily broad breach notice requirements based on the language of the statute.

Second, OTI argues against the type of harm trigger found in the overwhelming majority of state breach notice laws on the basis that "BIAS providers should not be making independent decisions about whether to notify their customers based on any perceived potential future harm or based on some specific type of potential future harm."[17] This argument begs the question of what constitutes a "data breach." As explained in our opening comments, the proposed rule would treat as a "data breach" events that involve a very broad range of information as to which no other security legal framework requires notice.

OTI's argument does not consider the issue of over-notification. OTI writes: "[I]f . . . a data breach occurs because of an employee mistake or some other seemingly innocuous

[14] Comments of New America's Open Technology Institute, p. 9.
[15] *In re* Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, *Notice of Proposed Rulemaking*, FCC 16-39, WC Docket No. 16-106, ¶¶ 56, 256 (March 31, 2016) ("NPRM").
[16] *See e.g.*, Fair and Accurate Credit Transactions Act, 15 U.S.C. § 1681, *et seq.*, Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6506, Cal. Civ. Code § 1798.83(d)(1)(e)(iii).
[17] Comments of New America's Open Technology Institute at p. 42.

circumstance, then the provider can explain that to the customer and let the customer decide how to handle responding."[18] The text of the NPRM itself specifically notes that over-notification is a serious concern, and the FTC comments agree.[19] [cites] As the FTC staff's comments explain: "[W]hen consumers receive 'a barrage of notices' they could 'become numb to such notices so that they may fail to spot or mitigate the risks being communicated to them.'" [20] Moreover, a 2014 study by the Ponemon Institute found that of consumers who had been victims of a breach, 32% did nothing after receiving a notification, and only 18% took the action suggested in the notification.[21] Even when notice is limited to a breach of sensitive data, some recipients ignore notice.[22] Lastly, breach notice can be costly.[23]

OTI's comments fail to address the practicalities in the timing of breach notice. OTI argues that, "BIAS providers should . . . notify customers under the timetables proposed, not 'without unreasonable delay' or as 'expeditiously as possible.' Such unclear and flexible deadlines . . . would increase the likelihood of harm to customers and complicate a straightforward requirement that is not unduly burdensome."[24] The FTC flatly disagrees. It supports our Coalition's opening comments that the Proposed Rule's 10-day notice requirement to consumers (seven days to law enforcement) is far too short and may not allow companies sufficient time to conduct an investigation.[25]

---

[18] Comments of New America's Open Technology Institute at p. 42.
[19] NPRM, ¶ 128 (Recognizing the harms inherent in over-notification (or "notice fatigue")); FTC Comments, p. 32.
[20] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, p. 31.
[21] Ponemon Institute, *The Aftermath of a Data Breach: Consumer Sentiment* at 1, 5 (Apr. 2014). National Consumers' League's statement that even if some consumers ignore notices others will take steps to protect themselves (Comments of the National Consumers' League, pp. 24-26) fail to take account for the fact that in cases where there is no risk of harm there is nothing for consumers to protect themselves from.
[22] *Id*.
[23] *See 2016 Ponemon Cost of Data Breach Study: Global Analysis* (June 2016).
[24] Comments of New America's Open Technology Institute, pp. 42-43.
[25] Comment of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission, pp. 32-33.

Companies need adequate time to do a thorough and accurate investigation before notifying affected parties about a breach; complex breaches take time to investigate. It does not help anyone if businesses notify consumers prematurely with incorrect information. Commenters who argue that this time frame is appropriate have little or no experience themselves handling data breach response. What is more, much of the information covered by the proposed rule's definitions would create no material risk of harm to consumers, making this argument about risk of harm in the period simply irrelevant as to most of the data presently included in the definitions of CPNI and customer proprietary information.

Like our opening comments, the FTC comments recommend modifying the proposed breach notification requirements in key respects:

(1) the breach notification requirement should apply to a narrower range of data and not cover information such as persistent identifiers because these create no risk;[26]

(2) notice should not apply to good faith access by employees because this poses no risk to consumers;[27]

(3) the very fast notification deadline in the NPRM should be considerably longer.[28]

In-line with state breach notice laws, the deadline should be 45 days, unless the investigation requires more time to determine the scope of the breach and secure the integrity of the ISP's system. In our collective experience, a significant number of complex breaches investigated promptly by sophisticated forensic firms do take this long to remediate, investigate and then provide notification. Existing state data breach notification requirements reflect the collective experience of both industry and state authorities.

The FTC also observes correctly that including information about credit bureaus is relevant only in circumstances where the acquirer of the information could use the information

[26] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at p. 10.
[27] *Id* at p. 32.
[28] *Id* at pp. 32-33.

without other information to open a financial account in the name of the customer.[29] Accordingly, this requirement should not be imposed in all instances.

Finally, OTI also argues that ISPs should list specific security measures in notices to consumers.[30] This ignores that disclosing security measures that an entity employ can give hackers very valuable clues about how to attack that target.

IV. CONCLUSION

For all these reasons, we urge the Commission to revise its proposed rules' information security and security breach notice provisions to limit audit trail and access control requirements and data breach notice requirements to apply only to sensitive personal information. We also urge the Commission to align the breach notice requirements for sensitive broadband ISP customer data and for CPNI with state breach notice law requirements and exceptions.

Respectfully submitted,

/s/

Jim Halpert
Anne Kierig
Counsel to the State Privacy and Security Coalition, Inc.
DLA Piper LLP (US)
500 8th Street, NW
Washington, D.C. 20004
(202) 799-4441

[29] Comments of the Staff of the Bureau of Consumer Protection of the Federal Trade Commission at p. 34.
[30] Comments of New America's Open Technology Institute, p. 35.